

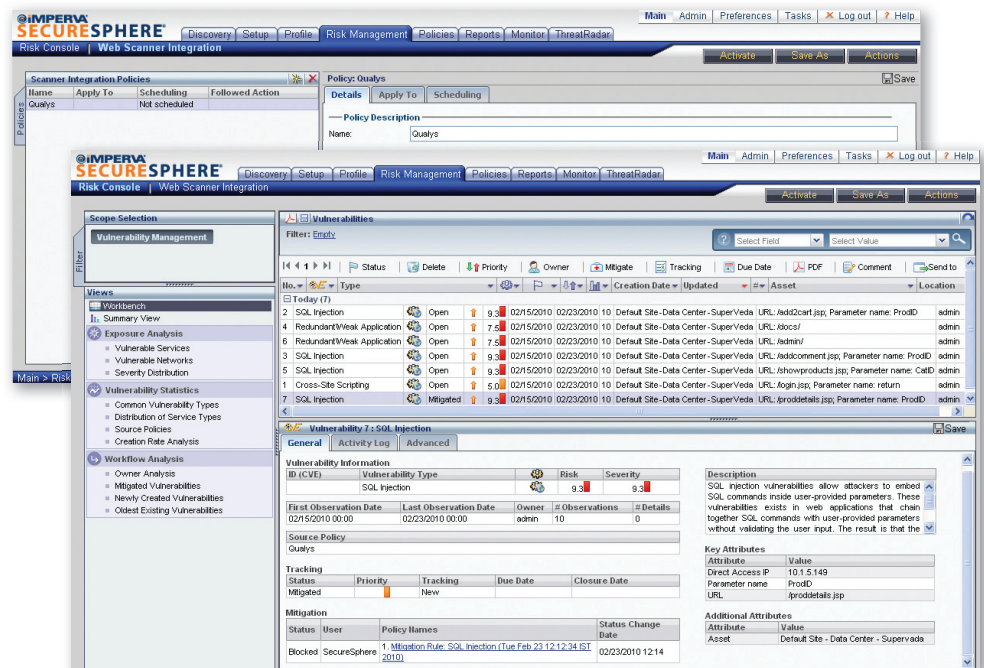
UNIFIED WEB APPLICATION VULNERABILITY ASSESSMENT AND VIRTUAL PATCHING WITH QUALYS AND IMPERVA

The joint solution by Imperva and Qualys improves visibility for application developers and provides instant protection against vulnerabilities.

Organizations can now maintain optimal security while following the appropriate process for developing, testing, and deploying application patches.

In order to protect critical business applications, security vulnerabilities must be addressed as soon as possible. Many organizations build security measures into their Software Development Life Cycle (SDLC) by implementing a process to scan for Web application vulnerabilities. However, manually fixing applications after a scan can take several weeks or even months. Any delay in fixing vulnerabilities can increase the risk of exploitation. Businesses are therefore forced to develop emergency fixes and tests, thus incurring significant operational costs and business disruption.

The integration of QualysGuard Web Application vulnerability scanner and Imperva's SecureSphere Web Application Firewall (WAF) significantly reduces the need for disruptive patching of vulnerabilities. Organizations can use QualysGuard to scan their Web applications for vulnerabilities and then import the scan results into SecureSphere WAF. SecureSphere WAF provides instant mitigation for imported vulnerabilities using a "virtual patch," which limits the window of exposure and reduces the security risk on the business.



The screenshot displays the Imperva SecureSphere WAF interface, specifically the Vulnerability Management section. The interface shows a list of vulnerabilities imported from QualysGuard. The selected vulnerability is 'Vulnerability 7: SQL Injection', which is shown in detail with its CVE, type, risk, severity, and description. The interface also shows the tracking and mitigation status of the vulnerability.

No.	Type	Status	Creation Date	Updated	Asset	Location
1	SQL Injection	Open	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /addCart.jsp; Parameter name: ProoID
2	Redundant/Weak Application	Open	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /hccol/
3	Redundant/Weak Application	Open	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /admin/
4	SQL Injection	Open	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /addcomment.jsp; Parameter name: ProoID
5	Cross-Site Scripting	Open	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /showproducts.jsp; Parameter name: CatID
6	SQL Injection	Open	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /login.jsp; Parameter name: return
7	SQL Injection	Mitigated	02/15/2010	02/23/2010	Default Site-Data Center-Super/Veds	URL: /prodDetails.jsp; Parameter name: ProoID

Vulnerability 7: SQL Injection

General | **Activity Log** | **Advanced**

Vulnerability Information

ID (CVE)	Vulnerability Type	Risk	Severity
SQL Injection	SQL Injection	9.3	9.3

First Observation Date: 02/15/2010 00:00
Last Observation Date: 02/23/2010 00:00
Owner: admin
Observations: 10
Details: 0

Source Policy: Qualys

Tracking

Status	Priority	Tracking	Due Date	Closure Date
Mitigated	New	Tracking		

Mitigation

Status	User	Policy Names	Status Change Date
Blocked	SecureSphere	1 Mitigation Rule: SQL Injection (Tue Feb 23 12:12:34 IST 2010)	02/23/2010 12:14

Description: SQL injection vulnerabilities allow attackers to embed SQL commands inside user-provided parameters. These vulnerabilities exist in web applications that chain together SQL commands with user-provided parameters without validating the user input. The result is that the

Key Attributes

Attribute	Value
Direct Access IP	10.1.5.149
Parameter name	ProoID
URL	/prodDetails.jsp

Additional Attributes

Attribute	Value
Asset	Default Site - Data Center - Superveds

QualysGuard scan results are imported into SecureSphere WAF. Using Imperva WAF's Virtual Patching, customers can quickly mitigate against discovered vulnerabilities.

Unified Web Application Vulnerability Assessment and Virtual Patching with Qualys and Imperva

About Imperva

Imperva, the Data Security leader, enables a complete security lifecycle for business databases and the applications that use them. Over 4500 of the world's leading enterprises, government organizations, and managed service providers rely on Imperva to prevent sensitive data theft, protect against data breaches, secure applications, and ensure data confidentiality. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring from the database to the accountable application user and is recognized for its overall ease of management and deployment. For more information, visit www.imperva.com.

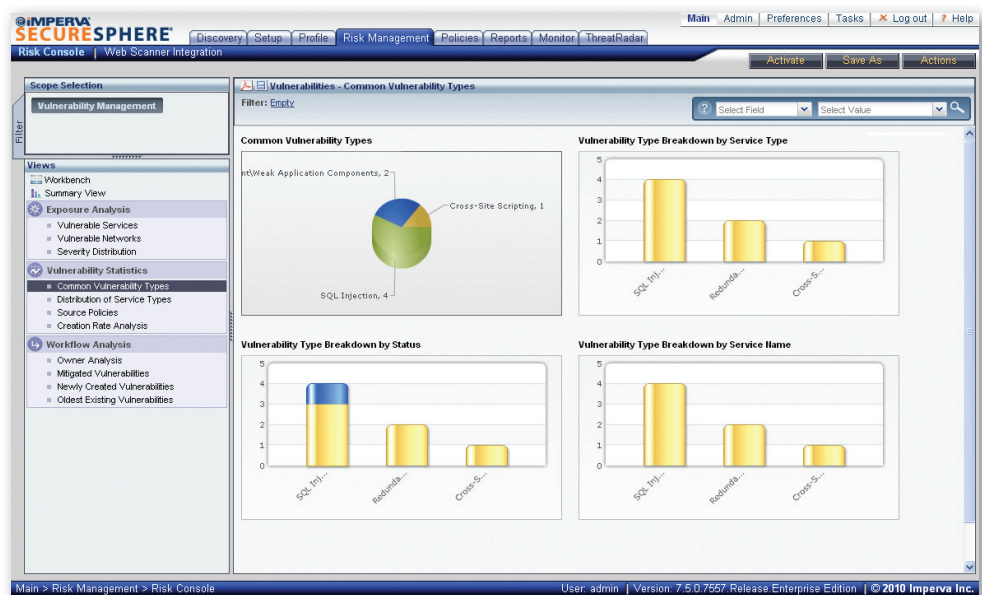
About Qualys

Qualys, Inc. is the leading provider of on demand IT security risk and compliance management solutions – delivered as a service. Qualys' Software-as-a-Service solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures.

The QualysGuard® service is used today by more than 4000 organizations in 85 countries, including 42 of the Fortune Global 100 and performs more than 250 million IP audits per year. Qualys has the largest vulnerability management deployment in the world at a Fortune Global 50 company. Qualys has established strategic agreements with leading managed service providers and consulting organizations including BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, NTT, SecureWorks, Symantec, Tata Communications, and TELUS. For more information, please visit www.qualys.com.

The Imperva SecureSphere WAF integration with QualysGuard provides customers with the following benefits:

- **Eliminates emergency fix and test cycles:** immediately remediates discovered Web application vulnerabilities via a “virtual patch” without the need for ad-hoc development intervention.
- **Reduces the window of exposure:** protects against Web application vulnerabilities while enabling organizations to follow their normal process of thoroughly testing and applying patches.
- **Prioritizes Web application firewall alerts:** eliminates false positives based on accurate, verified security risks identified by QualysGuard.
- **Generates accurate security and compliance reports:** highlights attempts to exploit known vulnerabilities.
- **Granularly manages security vulnerabilities:** imports specific types of QualysGuard application assessment results to the SecureSphere WAF based on severity level or class.
- **Exceeds the minimum PCI DSS 6.6 requirements:** provides the best protection available against data compromise.



The Imperva and Qualys integration improves visibility and provides immediate protection against Web application attacks.



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • Beechwood House, 2nd Floor, 10 Windsor Road, Slough, Berkshire, SL1 2EJ • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • P.O. Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

